DID YOU KNOW

OSHA issued new recordkeeping and reporting requirements in September, aimed at helping employers focus on preventing fatalities and other serious injuries.

In this month’s newsletter, we look at some of the major changes brought about by the new OSHA rule and provide a flowchart to help you keep track of your new reporting responsibilities.

New Reporting Requirements from OSHA

In early September, the Occupational Safety and Health Administration (OSHA) announced a final rule that requires employers to notify OSHA within eight hours after an employee is killed on the job. The rule also requires notification within 24 hours when an employee suffers a work-related hospitalization, amputation or loss of an eye.

The previous regulations only required notification of work-related fatalities and inpatient hospitalizations of three or more employees.

OSHA has also updated the list of industries that are exempt from the requirement to regularly keep injury and illness records. The industries are exempt due to having relatively low occupational injury and illness rates.

Details of the new requirements and the list of exempt industries can be found at www.osha.gov/recordkeeping2014.

New Week, New Data Breach

Target. Home Depot. Jimmy John’s. Lately it seems as though we are hearing about a new data breach practically every week.

Well, it turns out there is a reason for this deluge of data breach-related news. According to a new report from the Ponemon Institute, 43 percent of companies have experienced a data breach in the past year. That is a 10 percent jump from the year before.

A data breach can result in devastating financial and reputational consequences. As a result, more and more businesses are looking for protection in the form of cyber liability insurance.

(Continued on next page.)
The exposures that cyber liability insurance can protect you from differ from business to business, and every policy is tailor-made for each business, but typical data breach exposures covered by a cyber liability policy include:

- Notification of affected customers
- Crisis management
- Fixing your IT security
- Identity theft protection for affected customers
- Protection from potential legal action

The effects of a data breach can be far-reaching and last longer than expected. Be sure your business is protected by contacting Baldwin Krystyn Sherman Partners today.